# CS3072/CS3605 Final-year Project: Task 1 - Project Synopsis

|  |  |  |  |
| --- | --- | --- | --- |
| **Student** **Number** | 1516552 | **Supervisor** | Mark Perry |
| **Programme** |  | **Specialism** |  |
| **Provisional Title** | Exploring the effectiveness of ways to make a ‘strong’ password | | |
| **Problem Definition** | | | |
| Since Passwords are the most common means of protection and authentication of online accounts, there have been more and several ways of cracking the password than strengthening it. Therefore, the problem I will be addressing in this project is to investigate the ways to create a strong password, with a clear outline of what is considered ‘strong’ for a password and how it holds against the modern password cracking methods.  Some of the recommendations according to ‘webopedia’ for making a strong password is to simply increase the password length from an average 6-8 Characters to 11-12 Characters, make use of symbols, upper and lower case letters and so on.  Through this project, I will be exploring various ways and recommendations of heightening the security of passwords in consideration with more algorithms and toolkits being designed to crack passwords with tools such as PCFGs and hidden Markov Models. | | | |
| **Aims and Objectives** | | | |
| Aims   * Shed light upon the negligence of guidelines and rulesets for creating a strong password by end users. * Investigate the safety of passwords is indeed dependable on how fast the selected cryptographic functions can calculate hashed password. * Explore How secure is the password securing methods used by commonly visited websites? Hash functions? Encryption?’ will be investigated alongside the different password cracking techniques and how it holds against the current practice of strengthening the password. * Arrive to a conclusion and make recommendations implementing the techniques discussed in this project.   Objectives   * Test password implemented with rulesets recommended to make it strong using the different password cracking methods and evaluate how effective is the ruleset at keeping the password from being cracked. As most or all passwords can be cracked since it is a matter of when and not how. * Have a small focus group create login credentials to obtain passwords that the users think is ‘strong’ versus the password made secure through the current recommendation. i.e. 11-12 Characters, symbols, upper and lower case letters and so on. * Use the two obtained passwords from the research phase and test it against the password cracking methods. * Investigate the different attacks such as brute force, dictionary, rainbow table etc. and shed light upon the efficiency of these attacks at cracking the password that has been made secure through various addition of rulesets. * Explore the potential of future attacks with the ever so progressing GPUs and how the current practice of secure password will hold its ground. * Explore the literature of human-factor side of a secure password generation. * Investigate online password generators and the password creation policies of major social networking websites. | | | |
| **Background Sources** | | | |
| In order to “Explore the effectiveness of ways to make a password ‘secure’ “, I will be researching variety of background sources which will mostly be related to Password security.  The Problem of password security has existed from as early as the 1960’s when the first password was invented by the man named ‘Fernando Corbato’. However, the man himself has commented on the security of password as being a “kind of a nightmare” in an interview with The Wall Street Journal. The password is “vulnerable by nature” as said by ‘Jonathan Klein’, a president of a mobile identity solution for enterprise company. Hence, why I will be looking into various ways of making a password secure and how they hold against the attacks such as brute force, dictionary attack and so on.  The incentive for my project came from a similar yet different scope oriented project conducted by an undergraduate student of University of Oxford who explores the area of password vulnerability and its “resistance to an ‘everyday’ attacker”. | | | |
| **Approach** | | | |
| The Project Management Methodology I will be using will be a ‘Waterfall Methodology’. I found this the most suitable and efficient for my project specifically because with this method, the planning is everything which sets the foundation and foreshadows the outcome of the project. This approach will give me a realistic prediction of end result, timeline and scope.  The ‘Requirements’ are laid out in the beginning in full which cascades the workflow like a waterfall through different phases of the project. The importance of completing the given task before moving onto next phase which means the outcome of one phase sequentially acts as an input for the next phase will ensure the details and the literature of the context is kept under scrutiny.  In terms of ethical considerations, acquired data such as copies of cracked hashes and rainbow table of password hashes are readily available in public domain. Therefore, it does not increase nor affect the knowledge of passwords to the rest of the public.  However, I will be conducting a focus group to obtain the kind of passwords that general public thinks are strong which will be hashed at all times and no information about individuals will be revealed which will require me to go through the ethical process of BREO system for Brunel University. | | | |
| **Evaluation** | | | |
| The results that will arise from this project will give me an insight on how passwords can be made stronger with the importance of user training which is mostly neglected in password security field. Through the outcome of this project I will be able to evaluate the current practice of creating a ‘strong’ password and assessing if it really is secure enough to hold its ground against the current available password cracking methods.  However, with the ever so advancing GPUs which will be able to crack much more passwords per millisecond as opposed to now, raises the importance of user training compared to creating stricter password creation policies and having a password manager. | | | |